Control Systems Field Equipment Forensics

What happened to my PLC and how do I fix it?

Raymond C. Parks

Senior Member of Technical Staff

Sandia National Laboratories

Assurance Technologies and Assessments Department

Sandia is a multiprogram laboratory operated by Sandia Corporation, a Lockheed Martin Company, for the United States Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000. SAND2010-7220C

Sandia National Laboratories

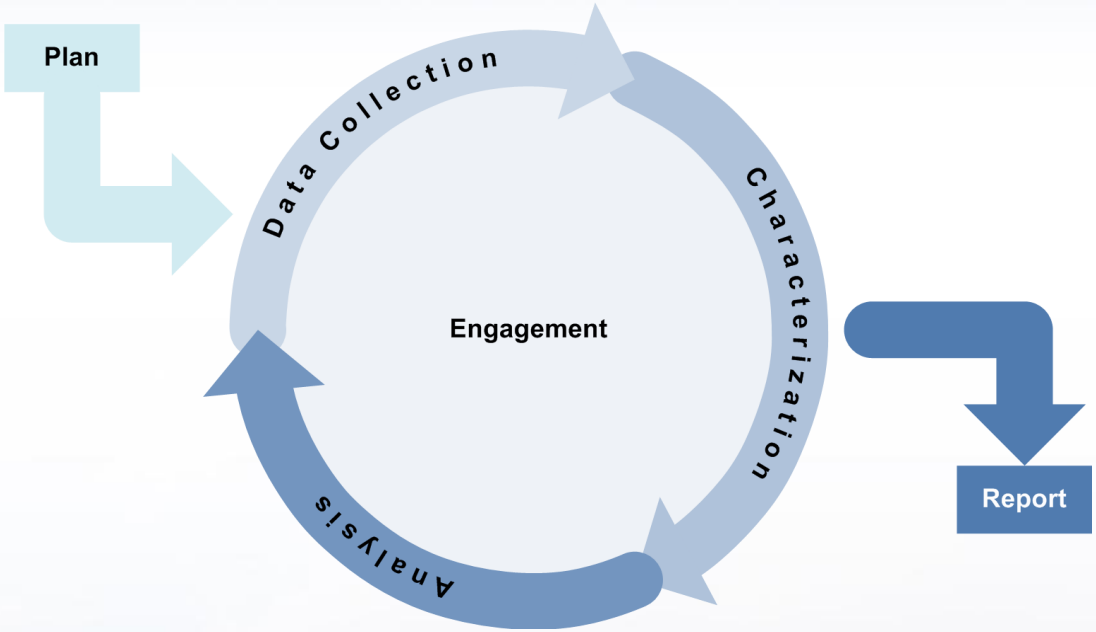
Outline

- **Advance preparation**
  - Think about attacks before they happen
  - Configuration Management
  - Backups
  - Off-site storage
  - Design and build for resiliency
  - Training operators to detect attack
- **Detection**
  - How do I know I've been attacked?
  - The front-line detection system - operators
- **Triage**
  - Working through the attack
  - Law enforcement or business continuity
  - Deciding what to fix first
- **Field Equipment Forensics**
  - Engineering Workstation
  - Projects/Configurations/Programs
- **Conclusion and Discussion**

Advance Preparation

- **Think about attacks before they happen**
  - Borrow from the military - Intelligence Preparation of the Operating Environment
  - Red team your process and your control system – figure out what is likely to be attacked by whom
  - Use your own engineers and operators – they know about past failures and have thought of possible attacks
  - Decide the relative risk of attacks
  - Estimate the consequences/cost of attacks for future use
  - Record and know the costs of recovery from previous normal/abnormal/malevolent events
  - Develop contingency recovery plans for malevolent events – start with your existing contingency recovery plans

IDART to anticipate attacks

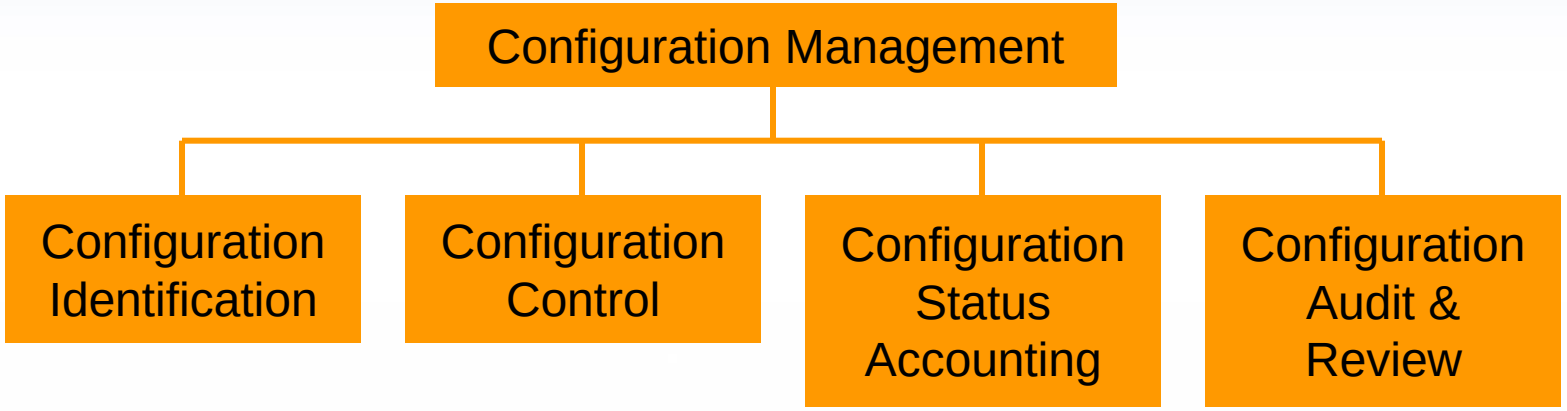


Use red-teaming to
anticipate your adversary

"Victorious warriors win first and then go to war, while defeated warriors go to war first and then seek to win."

Sun Tzu, *Art of War*

Advance Preparation



- **Configuration Identification – find out what you have**
  - Complete list of what you have where
    - Hardware, Software, Configurations, Licenses, Security files, Cables, Communications
- **Configuration Control – change only with the right authority**
- **Configuration Status Accounting – keep track of what you have**
- **Configuration Audit – check on yourself**

Advance Preparation

- **Backups**
  - Configuration management of field equipment only lets you know what it should be – that let's you reconstruct it from scratch
  - It's better to have backups of what your field equipment should be (hardware and software) ready to replace systems that have been attacked
  - Software - Common Operating Environment, Disk images, Specialized configuration information
  - Control system - HMI, Points, Ladder logic, PLC/RTU/IED configuration (network downloadable or serial capture)
  - Network
    - IP network -Switch, router, firewall configurations
    - Serial network - Ports and device mappings
  - Communication - paths and configurations
    - Internal telecom
    - External telecom

Advance Preparation

- **Offsite Storage**
  - On-site backups are convenient, but offsite is harder for an adversary to attack
  - If you stick with on-site, keep the backups away from networks and strictly control physical access
- **Most of the backup info can be digital**
  - Store it someplace far away in physical space
  - It's still close by in cyber space

Advance Preparation

- **Diagrams and Pictures - Disaster recovery that helps with field equipment incident response**
  - Remember, your network is an asset
    - Make sure you know your network
    - Have diagrams of the IP network and the serial network
  - Boring pictures and movies can be important
    - Take digital pictures of your equipment in place
    - Make movies showing equipment with commentary by engineers familiar with that equipment
    - Store these with your off-site backups
  - Not all attacks will be cyber-only – you need to make sure the field equipment is hooked up the way you intended

Advance Preparation

- **Design for resiliency**
  - Many control systems have resilient design elements
    - Dual networks
    - Redundancy
    - Safety systems
  - Resilient against equipment failures or abnormal events is not the same as resilient against attack
    - Dual networks provide two paths of attack
    - Redundancy means the same attack is performed twice
    - Safety systems are a control surface – if they can't be easily attacked
  - Heterogeneous redundancy provides normal/abnormal/malevolent resilience – both in networks and equipment
  - Separate safety systems from both control and business networks
  - Support configuration management with system like OPSAID
  - Design protections or recovery for highest risk attacks

Advance Preparation

- **Training operators to differentiate an attack from a malfunction**
  - Borrow from the military - Intelligence Preparation of the Operating Environment
  - Red team your process and control system – figure out what is likely to be attacked by whom
  - Simulate that attack – in your control system trainer or with the trainer that Sandia developed for I3P
  - Train your operators against attack events

Detection

- **How do I know I've been attacked?**
  - Attacks look like abnormal or even normal problems in control systems
  - Look for indicators – BSOD, persistence, changing malfunctions
  - Use resilience from redundancy to detect – replace possibly bad with known good
  - Get physical reading of points and compare to control system
  - Compare safety system readings to control system readings

Detection

- **The front-line detection system – operators**
  - The first line of defense against attack is the operators at the controls
  - Operators will notice the changes in the process that result from an attack
  - Operators will notice the changes in the control system that result from an attack
  - Outside operators can help with physical readings to compare with the control system readings the inside operators get

Triage

- **Working through the attack**
  - Critical first decision – bring things to a stop or try to keep going
    - Know in advance the cost of stopping – C_s
    - Assess quickly the possible consequences/cost of continuing to operate and failing to stop the attack - C_A
    - Estimate the chances of attack success - P_A
    - If P_A x C_A is greater than C_s – then hit the big, shiny red button
- **Law enforcement or business continuity**
  - Forensics to find out what's wrong and fix it is far different from forensics to provide evidence to law enforcement
  - If you have sufficient hardware and software back ups, you can consider preserving the evidence for law enforcement

Triage

- **Deciding what to fix first**
  - When normal/abnormal events happen, the system most important to the process has priority
  - When malevolent events happen, fixing the most important system may be a waste of time – it will just get re-infected from an ancillary system
    - Decide, using your contingency recovery plan, the minimum system you need
    - Remove everything except the minimum
    - If that doesn't get rid of all the ancillary systems – fix them first
    - Fix the most important system once you're sure it won't get re-infected
  - Importance may be determined by ability to operate manually
    - A cyber attack can't overcome shifting to manual operations
    - If you can sustain manual operations long enough, you have more flexibility about what to fix and when

Field Equipment Forensics

- **Look for evidence of reconnaissance**
  - Remote dial-up access – the stealthiest method of reconnaissance
    - Line-sharing switch logs – LSS are frequently used to share access to field equipment configuration ports with a telephone
    - Telephone calling records and complaints – possible evidence of war-dialing
  - Physical access – highly probable form of reconnaissance
    - Video records (tapes or, more likely, DVR)
    - Access logs – written (unlikely to show anything) or digital
    - Alarm history – especially alarms dismissed

Field Equipment Forensics

- **Look for evidence of reconnaissance (continued)**
  - Network access – to control center and field equipment containing information about control system and process
    - Firewall logs of all accesses (granted or denied) to relevant subnets – depending upon the level of logging set at the firewalls
    - Router logs (netflow) of packets routed to relevant subnets
    - Control center server logs of all access (granted or denied) to servers with relevant information
    - Intrusion Detection System events (OPSAID can help) that might indicate attacks to gain access and collect information on field equipment configuration – against the equipment, servers, or engineering workstations
  - Equipment access – if possible, check for access attempts and/or logs on the field equipment

Field Equipment Forensics

- **Configuration – check for evidence of changes to the configuration of the field equipment by comparing the actual field equipment configuration to a selection of reasonable configurations. If the actual does not match any of the reasonable configurations, there may have been tampering**
  - Obtain standard configuration from vendor
  - Obtain intended configuration from backups
  - Obtain as-build configuration from integrator
  - Obtain configuration from suspect field equipment
    - Use a known-good engineering workstation (build from scratch and don't connect to any possible sources of infection)
    - Connect to configuration port of suspect field equipment (over network or serial)
    - Use model specific method to show configuration
    - Capture the configuration (save to file, save to project, screen buffer for command line, save web-pages, etc.)

Field Equipment Forensics

- **Configuration – (continued)**
  - Compare target configuration to vendor default, as-build, and/or intended configurations. If it doesn't match any of these, someone may have tampered with it. Alternately, an engineer may have made changes without documenting them.
  - Analyze any discrepancies for a possible attack pattern.

Field Equipment Forensics

- **Firmware – field equipment acts upon their configuration through software stored in read-only memories or firmware. Vendors provide updated firmware images that can be installed through various means.**
  - Obtain a reasonable range of firmware images from the vendor and/or integrator. Images released from the equipment manufacture date all the way up to the current date may all be necessary depending upon the frequency of maintenance updates
  - Obtain the intended firmware version number from the configuration management system of the owner/operator
  - Obtain the firmware image from the suspect field equipment

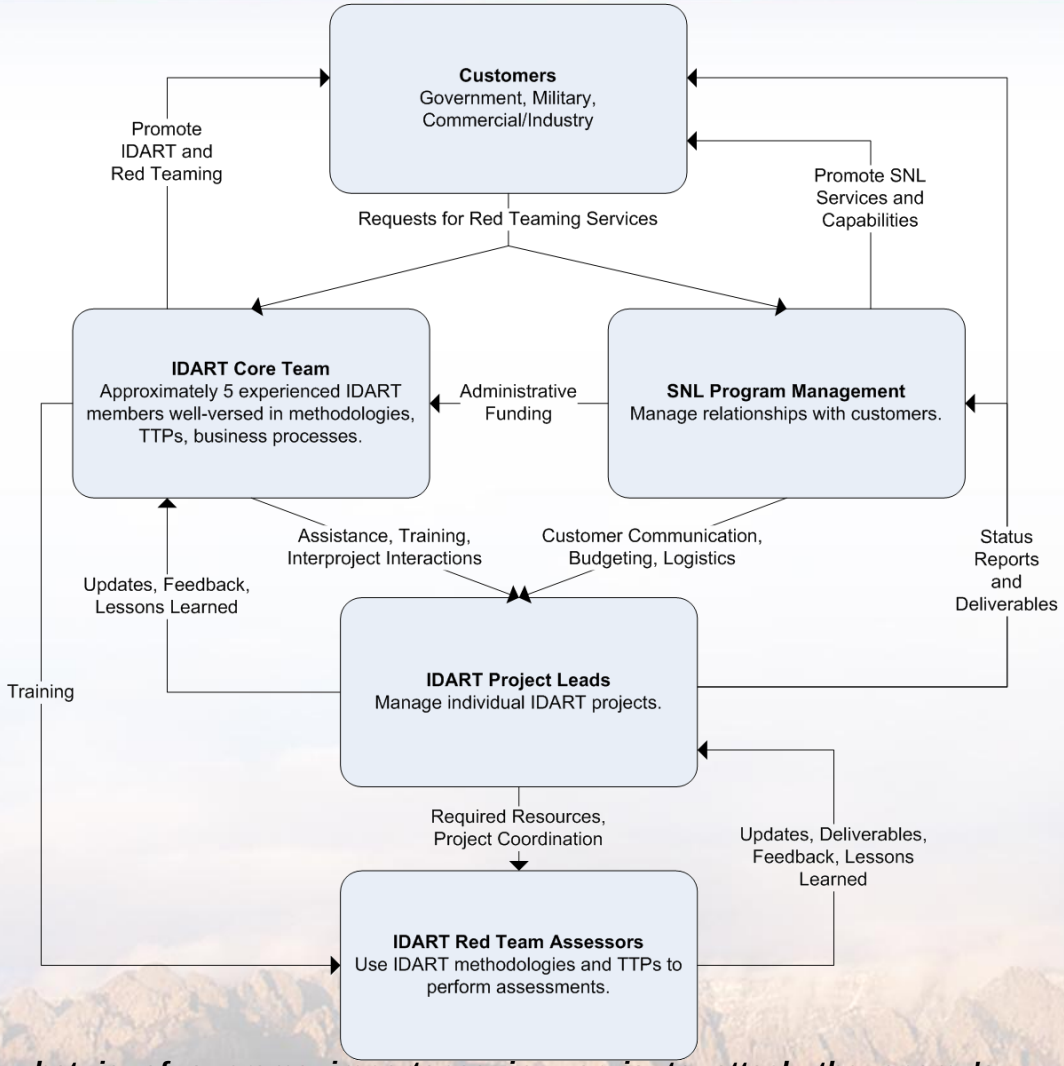
Field Equipment Forensics

- **Firmware – (Continued)**
  - Obtain the firmware image from the suspect field equipment
    - Download firmware image via configuration interface if possible.
    - The rest of these could be destructive testing due to damage to conformal coating and derating for environment/safety -
      - Use existing Joint Test Action Group (JTAG) port or solder port to JTAG pad. FPGAs and firmware in field equipment are frequently accessible from JTAG ports – even if the header is left off operational equipment a header can be added to the pad or there may be JTAG signal access using test points
      - Use clamp-on device to read flash memory. Firmware in field equipment is frequently stored in surface-mount flash memory chips. There are clamp-on devices that can be used to read surface-mount flash memory chips.
      - Remove and place flash or ROM into reader and read. Older field equipment may have firmware in removable memory. These can be removed, put in special readers, read, and then replaced with no harm to the field equipment.

Field Equipment Forensics

- **Firmware – (Continued)**
  - Compare hashes or checksums of firmware from suspect field equipment against the hashes or checksums of various vendor firmware images. If there is a match, compare that version number to the intended firmware version number. If there is no match, further analysis is necessary.
  - Binary diff firmware images - even if the firmware hashes or checksums match, the algorithm used may allow modification without detection. A full comparison of the two binary files - called a diff in computer science - is necessary to be sure in the case of weak algorithms. The binary diff is the first step in analyzing non-matching firmware checksums to find the instructions that are different.

IDART Structure and Operation



"Thus, what is of supreme importance in war is to attack the enemy's strategy."

Sun Tzu, *Art of War*

Overview of IDART Methodology

- **Plan – Understand what analysis is to solve**
  - Determine adversaries and nightmare consequences.
  - Negotiate constraints and boundaries, gather resources.
- **Data Collection – Derive adversary goals**
  - Gather system mission/requirements documents, designs, configuration information, security environment data, etc.
- **Characterization – Derive target opportunities**
  - Understand system components and dependencies
  - Develop views for discussion and validation purposes.
- **Analysis – Answer analysis questions with replicable results**
  - Consequence – What could happen after a successful attack?
  - Vulnerability – Where is the system weak against attack?
  - Attacks – What series of vulnerabilities must be successfully exploited to achieve adversary objectives?
  - Security performance – How does system perform under attack?

"In war, numbers alone confer no advantage."

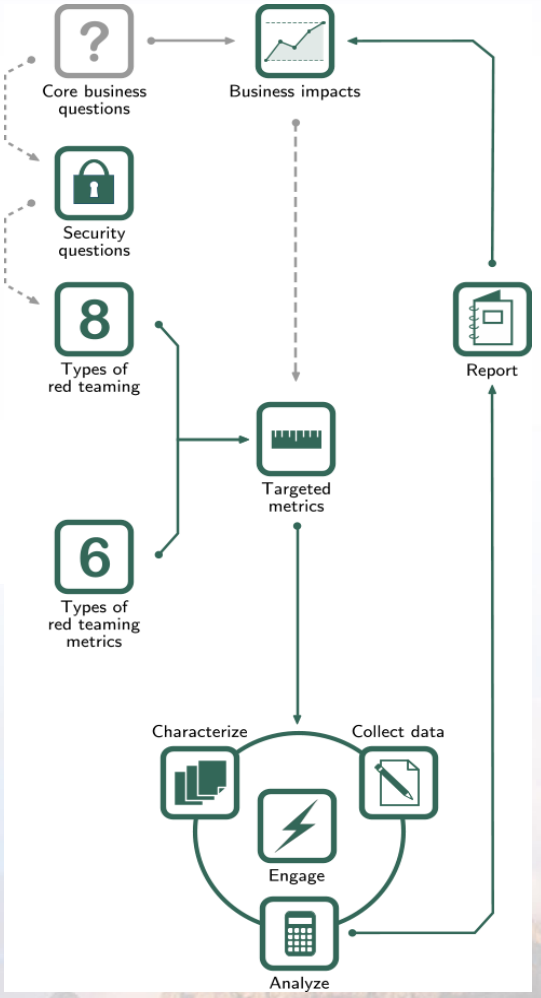
Sun Tzu, *Art of War*

IDART Operational Red Teaming Principles

- Stay legal
- Do no harm[1]
- Stay inbounds
- Maintain control
- Be able to prove your actions
- Ensure OPerations SECurity

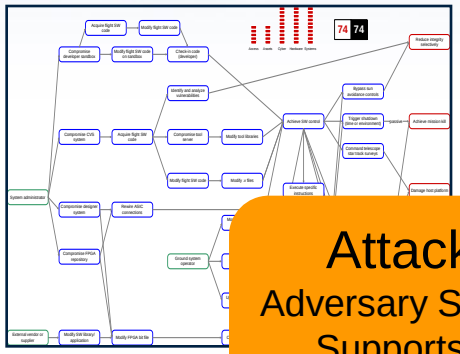
1. Any harmful action must be temporary or executed against test systems.

Red Team Metrics Process Overview



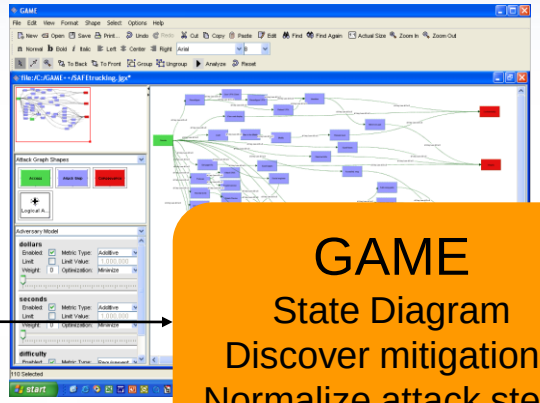
- The process maps to roles and responsibilities for THE SPONSOR and the REDTEAM.
- The RED TEAM LEAD has the biggest role in the use of this process

Expressing Attacks



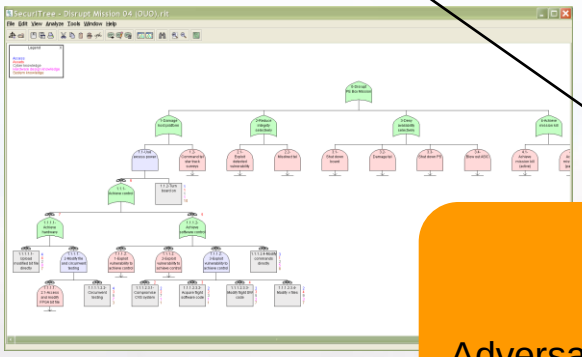
Attack Diagram

Adversary Sequence Diagram
Supports brainstorming
Communicates



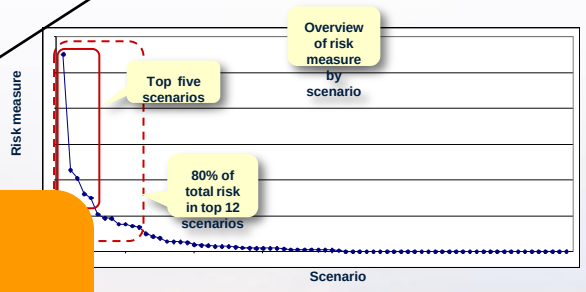
GAME

State Diagram
Discover mitigations
Normalize attack steps



Securitree

Fault-tree like
Adversary requirement modeling
Determine system effectiveness



Conclusion and Discussion

- **Red teaming works for supply chain**
  - Finds the worst attacks across multiple dimensions.
  - Shows where to best expend resources to reduce risk.
  - Provides positive control of potentially negative activities.

Raymond C. Parks
Senior Member of Technical Staff
Sandia National Laboratories
Assurance Technology and Assessments Dept.
rcparks@sandia.gov
(505) 844-4024

"To fight and conquer in all our battles is not supreme excellence; supreme excellence consists in breaking the enemy's resistance without fighting."
Sun Tzu, *Art of War*

References

[1] US Army Training and Doctrine Command. http://www.tradoc.army.mil/pao/tnsarchives/July05/070205.htm

[2] SANS Institute InfoSec Reading Room. http://www.sans.org/reading_room/whitepapers/auditing/red_teaming_the_art_of_ethical_hacking_1272?show=1272.php&cat=auditing

[3] Sandia IDART. http://idart.sandia.gov

[4] Duggan, D., *et. al.* Categorizing Threat: Building and Using a Generic Threat Matrix. 2007. Available: http://idart.sandia.gov/methodology/materials/Adversary_Modeling/SAND2007-5791.pdf

Control System Red Teaming - Planning

- **Planning**
  - Legal authority
  - Resources
    - All the usual plus critical infrastructure and ACS experts
  - Rules of engagement
    - Scope, clearance/access, recovery, trusted agent
  - Depth and breadth
  - Information protection
  - Consequences and adversary model
    - Loss of life, loss of service, loss of equipment, loss of money
    - Three types of consequences -
      - Consequences as flags
      - Consequences to collateral participants
      - Consequences to red team - safety
  - Safety and liability

Control System Red Teaming - Safety

- **Control Systems are in industrial environments**
  - Safety is mandated - OSHA
- **Safety is a real concern**
  - Dropping
  - Falling
  - Poisons
  - Radiation
  - High voltages
  - Confined spaces
- **New red-team equipment - besides laptops**
  - Steel-toe boots
  - Radiation badges
  - Hard-hats
  - Respirators

Control System Red Teaming - Tools

- **Active tools can be dangerous**
  - Why do you need to use an active tool?
  - Can you get that information some other way?
- **Real world examples**
  - Robot arm
  - Wafer Fab
  - Gas utility
- **Data mining tool for network topology discovery**
  - We use ANTFARM
    - Accepts data from many sources
    - Models network topology
    - Limit data collection to passive methods